Office of Financial Institutions
REMOTE ACCESS TO INTERNAL NETWORKS

I. Purpose:

Advances in technology, coupled with the popularity of telecommuting, performing work-related tasks from one's home or providing remote system maintenance/support have resulted in an increased need for remote access to OFI internal networks. Although remote access saves time and money, it also increases the risk of exposing internal networks to viruses, worms, spyware and unwanted eavesdropping or monitoring. Due to the wide range of remote access configurations and control (ownership), this policy and associated requirements are based on the assumption that remote access devices (desktop PC's, laptops) may be contaminated.

II. Policy:

OFI will allow remote access to their internal network, via desktop PC's and laptops by utilizing the secure application of GoToMyPC. OFI IT will ensure these devices are configured as indicated by the following Remote Access Requirements matrix.

Remote Access Requirements

	Access via Public Internet (ISP) (DSL, cable, dial-up, wireless)	Direct Dial-In (RAS, etc.)	Dedicated Circuit (point-to-point)
Contractor	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, dial-back, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only
Employee (on the road w/agency laptop)	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software w/ latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, 2-factor authentication, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	
Employee (home)	AV software w/ latest signatures, Personal FW, VPN, Spyware removal software/service with latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, dial-back or 2-factor authentication, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only	AV software w/ latest signatures, Personal FW, Spyware removal software w/latest signatures, latest security updates for the Operating System and the Internet browser, and restrict access to approved resources only

Note:
If and when access is allowed via VPN, the client software will be OFI-supplied.

Antivirus (AV) and personal *firewall* (FW) software on non-state-owned input devices is the responsibility of the user. However, this software is not vendor-specific, but must be a current product with the latest updates/virus signatures.

III. Scope:

This policy is applicable to OFI IT under the authority of the Office of Information Technology, pursuant to the provisions of R.S. 39:15.1, et seq.

IV. Responsibilities:

A. OFI IT will pursue the use of "health-check" software that determines the status (whether or not AV and FW software are loaded with the latest updates) of remote PC's and laptops before they are allowed access to the internal network.

B. Relative to development and support contracts, OFI will include specific contract language that requires the contractor to adhere to OFI IT Policies if there is need for remote access to the agency's internal network.

C. Blackberry/PDA devices and "smart phones", due to their fast-paced technological advances, are not within the scope of this policy. However, OFI IT must assess and take the necessary steps to mitigate the security risks associated with these devices.

APPROVED BY:

John Ducrest

May 9, 2008

John Ducrest, CPA
Commissioner

Date

This information was extracted in part from the Office of Information Technology Policy IT-POL-012 Remote Access to internal networks.